DISTRIBUTION
Central Files (A-47)
GIB Rdg
TASK File
SHanauer
FSchroeder
KKniel
PNorian
ASzukiewicz

MAY 19 1982

MEMORANDUM FOR: Karl R. Goller, Director
Division of Facility Operations

E. Wenzinger, Chief
Instrumentation and Control Branch
Division of Facility Operations

FROM: Stephen H. Hanauer, Director
Division of Safety Technology

SUBJECT: APPROVAL OF TASK ACTION PLAN (TAP) A-47
SAFETY IMPLICATIONS OF CONTROL SYSTEMS

The enclosed Task Action Plan of the Unresolved Safety Issues (USI) A-47, "Safety Implications of Control Systems" is being sent to you for concurrence prior to final approval.

This TAP has been developed by the Division of Safety Technology, NRR with input from various groups shown below. Earlier copies of this draft have been circulated within the NRC staff requesting comments. The comments have been incorporated and we believe that we have received agreement in resolving the comments. Comments (or a message that there were no comments) were received from:

F. Rosa/E. Rossi, NRR/DSI
M. Srinivasan/J. Knight, NRR/DSI
P. Jensen/F. Orr, NRR/DSI
J.T. Beard, SPEB/DL
E. Wenzinger/D. Basdekas, ICB/RES/DFO
B. Clayton, PTRB/DHFS
S. Newberry/F. Coffman, RRAB/DST
M. Chiramal, PSU/AEOD

The Task will perform an indepth evaluation of the non-safety grade control systems to verify the adequacy of current licensing design requirements and will propose (if necessary) additional guidelines and criteria to assure that nuclear plants do not pose an unacceptable risk due to control system failures.

Task A-47 will evaluate the non-safety grade control systems of three PWR designs and one BWR design. Two PWR designs (B&W and W) will be evaluated by ORNL under contract with the Office of Nuclear Regulatory Research. The BWR design will be evaluated by EG&G Idaho Falls under contract with NRR. The laboratory to evaluate the CE design will be determined later.

8206070028

OFFICE ▶						
SURNAME ▶						
DATE ▶						

OFFICIAL RECORD COPY

MAY 19 1982

The projected completion date for developing a draft NUREG for public comment is January 1984.

Please respond with your concurrence, concurrence with comment, or non-concurrence with reasons, on this form by May 27, 1982.

Stephen H. Hanauer, Director
Division of Safety Technology

Attachment:
TAP A-47

I concur _____

I concur with the following or attachment comment(s) _____

I do not concur for the following or attached reason(s) _____

OFFICE	DST:GIB	DST:GIB	DST:GIB	DST:AEGP	DST:D		
SURNAME	ASzukiewicz:cb	FMorlan	KKniel	FSchroeder	SHanauer		
DATE	5/13/82	5/17/82	5/17/82	5/17/82	5/19/82		

OFFICIAL RECORD COPY

Task A-47

May 1982

SAFETY IMPLICATIONS OF CONTROL SYSTEMS

Lead Organization:	Division of Safety Technology (DST)
Task Manager:	A. J. Szukiewicz, Generic Issues Branch (GIB)
Lead Supervisor:	Karl Kniel, Chief, Generic Issues Branch, DST
NRR Principal Reviewers:	C. Rossi, G. Mazetis, [illegible] Newberry, Division of Systems Integration; J. T. Beard, Division of Licensing; W.G. Kennedy, Division of Human Factors Safety-
AEOD Lead Reviewer:	M. Chiramal, Plant Systems Unit
RES Lead Reviewer:	D. Basdekas, Division of Facility Operations
Applicability:	Light Water Reactors (PWRs and BWRs)
Projected Completion Date:	January 1984

1. DESCRIPTION OF PROBLEM

Non-safety grade control systems are used to maintain the plant within the necessary pressure and temperature limits during normal shutdown, start-up, and load varying power operation. The control systems are not relied upon to perform any safety functions following postulated accidents but are required to control plant processes that could have a significant impact on plant safety. Those control systems include the reactivity control systems, and reactor coolant pressure, temperature, level, flow and inventory controls (e.g., borated water controls). In addition, they include secondary system pressure and flow controls (pressurized water reactor) as well as the associated support systems such as electric, hydraulic and/or pneumatic power supply systems.

During the licensing process, the staff performs an audit review of the non-safety grade control systems, on a case-by-case basis, to assure that an adequate degree of separation and independence is provided between these non-safety grade systems and the safety systems, and that effects of the operation or failure of these systems are bounded by the accident analysis in Chapter 15 of the plant's Safety Analysis Report (SAR). Typical events that are addressed by the licensees, and are evaluated by the staff in the audit review include, but are not limited to: 1) the feedwater system malfunctions that result in a decrease or an increase in the feedwater flow (including the loss of the normal feedwater flow); 2) the steam pressure regulator malfunctions or failures that result in an increase or a decrease in the steam flow (including the turbine trip event); 3) a spectrum of rod ejection accidents for pressurized water reactors (PWRs) and rod drop accidents for boiling water reactors (BWR), and 4) chemical and volume control malfunctions that increase the reactor coolant inventory or decrease the boron concentration.

On this basis it is generally believed that control system failures are not likely to result in loss of safety functions that could lead to serious events or result in conditions that the safety systems are not able to mitigate. In-depth studies for all the non-safety grade systems have not been performed however, and there exists some potential for accidents or transients being made more severe than previously analyzed, as a result of some of these control system failures or malfunctions.

The control system failures or malfunctions may occur independently or as a result of an accident or transient under consideration. Failures or malfunctions may also occur as a result of a common mode or a system interaction that could make recovery to normal safe shutdown conditions difficult.

Two potential concerns have already been identified in which a failure or malfunction of the non-safety grade control system can 1) potentially cause

a steam generator or reactor vessel overfill, or 2) can lead to a transient (in pressurized water reactors) in which the vessel could be subjected to severe overcooling. In addition there is the potential for an independent event i.e., a single failure, (such as a loss of power supply, a short circuit, open circuit; control sensor failure) or a common mode event (such as a harsh environment caused by an accident or a seismic event) to cause a malfunction of one or several control systems which would lead to an undesirable control action, or provide misleading information to the plant operator. These concerns will be reviewed and evaluated as part of the tasks discussed in the following sections. It should be recognized that the effects of control system failures during accident or normal plant operation may differ from plant to plant, and therefore it may not be possible to develop generic solutions to these concerns. It is possible, however, to develop generic criteria that can be used for the plant specific reviews.

The purpose of this Unresolved Safety Issue is to perform an in-depth evaluation of the control systems that are typically used during normal plant operation and to verify the adequacy of current licensing design requirements or propose additional guidelines and criteria to assure that nuclear power plants do not pose an unacceptable risk due to inadvertent non-safety grade control system failures.

2. PLAN FOR PROBLEM RESOLUTION

In order to best utilize NRC's capabilities and resources, the resolution of the activities described in detail in the following sections will be conducted under contract with the National Laboratories. The responsibility for resolution of this safety issue rests with the Office of Nuclear Reactor Regulation (NRR), but will involve both NRR and the Office of Nuclear Regulatory Research (RES) staff effort to manage and review the adequacy of the evaluations conducted. To scope the issue to a manageable level and bound the generic review to a reasonable completion schedule, Task A-47 will evaluate the non-safety grade systems of three PWR designs and one BWR design.

The task will review the plant designs of the manual and or automatic control systems for each of the four nuclear steam system (NSS) supplier designs [i.e., Babcock and Wilcox (B&W), Combustion Engineering (CE), General Electric (GE) and Westinghouse (W)] and will include the review of any manual and/or automatic control system that interfaces with the NSS design or dynamically interacts with the primary reactor fluid system and the secondary steam system. These associated control systems may be supplied or designed by different manufacturers or architect/engineers than the NSS supplier. Two PWR non-safety grade control system plant desings (i.e., B&W and W) will be evaluated by ORNL, under contract with the Office of Nuclear Regulatory Research (FIN No. B-0467). The General Electric BWR designs will be evaluated by EG&G Idaho under contract with NRR (FIN No. A-6477). The decision on where the CE evaluation will be performed is to be made later on the basis of progress at the two labs.

The Task will, for each type design: 1) identify the non-safety grade control system(s) whose failure or misoperation can, a) cause transients or accidents

identifyed in Chapter 15 of the Final Safety Analysis Report (FSAR) to be made more severe than previously analyzed, b) create the potential to negate the timely action of the automatic protection system or the manual operation of any equipment required to achieve a safe shutdown condition; 2) establish and define the order of importance of the control system(s) identified as having safety significance; 3) describe the mechanism(s) contributing to the failure modes, (e.g., loss of power supply or the environmental effects on the control systems); 4) verify the adequacy of the existing design criteria, described in Standard Review Plan (SRP) Section 7.7, or develop and propose additional criteria and guidelines to improve system reliability or minimize the consequences of the control system failures that have been identified as safety significant.

To evaluate control system actions that have safety implications, the work effort is sub-divided into the following tasks.

1. Evaluate control system failures that could cause a steam generator or a reactor vessel overfill transient.

2. Evaluate control system failures that could cause a reactor overcooling transient.

3. Evaluate (all other) non-safety grade control systems that have safety implications.

4. Evaluate the effect of loss of power supplies to the control systems. This would include the electrical AC and DC supplies also and the pneumatic and hydraulic supplies.

It is anticipated that the major effort will be in reviewing task 3 and 4. The review of task 1 and 2 is considered a specific sub-task of overall effort. These tasks and the scope of the sub-task activities are outlined below. Additional tasks or sub-tasks may be identified as the program develops, if other tasks are developed, the Task Action Plan will be revised. Should these reviews indicate that additional criteria for control system designs are necessary or that specific problems require resolution, appropriate action will be taken for plants in the licensing process and for plants now in operation.

Task Action Plan A-47 has been developed to utilize, whenever possible, any applicable data developed by the following current on-going activities.

1. Resolution of USI A-49 "Pressurized Thermal Shock" (PTS).

2. Office of Nuclear Regulatory Research activities with Oak Ridge National Laboratory regarding Safety Implications of Control Systems (FIN No. B-0467).

3. Systems Interaction Program - A study conducted by the Reliability and Risk Assessment Branch of the Division of Safety Technology (RRAB/DST). TMI Action Plan Item II.C.3 and USI A-17.

4. Office of Nuclear Regulatory Research - Activities with Sandia National Laboratories evaluating plant electrical systems interactions (FIN No. A-1324)

The interface between the Task A-47 program and these activities is discussed in more detail in the appropriate sub-tasks.

Task Descriptions

Task 1. EVALUATE CONTROL SYSTEMS THAT CAUSE STEAM GENERATOR (PWR) OR REACTOR VESSEL (BWR) OVERFILL TRANSIENTS.

This task will evaluate the non-safety grade control systems on each of the four plant designs (i.e., B&W, CE, GE, W) in order to identify any non-safety control systems whose failure could lead to a steam generator overfill (in a PWR plant) or a reactor vessel overfill (in a BWR plant). The control systems on three PWR plant designs, and one BWR plant design (to be selected) will be reviewed. The control system evaluation includes the design of the NSS supplier and also any control systems which may be designed by other suppliers that interface with NSS design, and dynamically influence the level of the reactor vessel or the steam generator. Recommendations in the form of guidelines or criteria will be developed (if necessary) for either control system modifications or for additional protection system functions which would minimize the consequences of control system failures or the transients that can lead to overfill. This task is considered a subtask of the broader task 3 activities and will consist of the following sub-tasks.

1.1 Identify the Systems Whose Failure Can Lead to Overfill

Conduct a review of the automatic and manual control systems and identify all systems that have the potential for causing a steam generator or reactor vessel overfill. Determine the potential impact on overfill for each of the systems that have been identified and establish the order of importance of these systems. Document the systems whose failure or malfunction may be considered less important or inconsequential to warrant any further study and document the basis of such action. During this stage, the criteria that will be used for selecting and categorizing the control systems whose failure may be of safety significance will be defined. A candidate criteria for identifying significant systems may be one whose failure or malfunctions may lead to water ingress (or significantly increase moisture carryover or steam quality) in the main steam line steam space. This water ingress may lead to a loss of safety systems (i.e., the loss of the auxillary feed pump turbines) or cause undue stress to the steam lines. Gross analysis such as qualitative FMEA on a system level basis will be used to identify these control systems. During this phase, non-mechanistic "worst-case" failure modes of the systems will be assumed. In addition, the major components of concern such as the valves, pumps, level transmitters, etc., whose failure can cause the specific system malfunction will be identified.

1.2 Identify System Failure Modes

Identify the failure mechanisms (i.e., causes) of the control systems that have been defined in sub-task 1.1. Mechanistic failure, such as short and open circuits, the loss of environmental support systems,

the loss of power supply (see task 4), seismic effects and operator action will be evaluated during this phase in order to determine the need and the type of corrective actions. Additional failure mode effects analyses (FMEA) and fault tree analysis will be performed on a component level for selected systems as needed. The need for the additional analysis will be evaluated on a case-by-case basis. The relative importance of the control system, its complexity, and its dependence on other systems will be a factor for implementing any additional analysis. During this phase, the review of the applicable portions of the subtasks described in task 4 (the effects of loss of power supplies) will be conducted on those control system designs, identified in Section 1.1.

1.3 Conduct Computer Simulation Studies for Combination of System Failures

Develop an analytical model to simulate the overfill transients using existing codes whenever possible. As part of the activities conducted at Oak Ridge National Laboratory (FIN B-0467), RES will develop a generic model to simulate the dynamic behavior of a PWR type plant. Concurrently, as part of the activities conducted at EG&G Idaho (FIN No. A-6477) we plan to develop a generic model to simulate the dynamic behavior of a BWR type plant. These models will include the plant characteristics of the primary reactors fluid system and the secondary steam and feedwater system, as well as the modeling for the major elements of the control systems. We plan to use these generic models, modify them as necessary to simulate the plant specific characteristics of the four plants under review, and evaluate the transients that would occur as a result of the system failures identified in sub-task 1.1. Appropriate combinations of these failed systems, in sequence and simultaneously, will be evaluated in these simulation studies. It is anticipated that this tool will significantly minimize the need for extensive use of the analytical techniques that normally would be used for the tasks identified in Sections 1.1 and 1.2 above.

1.4 Determine the Need for Control or Protection Systems Improvements

Evaluate the need for additional safety or non-safety grade equipment such as high level alarms, level controls, or interlocks (e.g., feedwater pump trips) or modifications on the existing designs. Also evaluate the need for additional improvements on the existing controls or electrical power system of the control systems identified in Section 1.1. The need for additional or improved operator action should be considered during this phase. Evaluate the effectiveness and the merits of each of these types of system modifications and establish the basis for a selection preference (i.e., high reliability, cost effectiveness, etc.).

1.5 Provide Design Criteria for the Evaluation of Control and or Protection Systems for Overfill

Verify the adequacy of the existing criteria for control systems (Standard Review Plan Section 7.7) or if necessary develop and propose additional criteria or guidelines to improve system reliability and minimize control system failures that could lead to steam generator or reactor vessel overfill.

As a result of this study and at the completion of this task, the NRC staff will issue an evaluation and propose, if necessary, any modifications to existing criteria. The report will contain proposed recommendations for future staff actions.

Task 2. EVALUATE CONTROL SYSTEM FAILURES THAT COULD CAUSE A REACTOR OVERCOOLING TRANSIENT.

This task will evaluate the non-safety grade control systems of three PWR plants and one BWR plant design (to be selected). The control system evaluation will review each of the four reactor vendor designs (B&W, CE, W, and GE) and will include the control systems on the specific plants which may be designed by other suppliers but interface with the NSS control system or interact with the primary system in a manner that could lead to an overcooling transient. The objective of this task is to identify those control systems whose failure or malfunction can contribute to an overcooling transient in the primary system of sufficient magnitude to initiate re-pressurization via the automatic initiation of the safety injection system.

Proposed recommendations in the form of guidlines or criteria will be developed (if necessary) for control system modification or for additional protection system functions which would minimize the impact of control system failures or malfuncitons that could contribute to significant pressurized overcooling transients. This task is considered a subtask of the broader task 3 activities and will consist of the following sub-tasks.

2.1. Identify the Systems Whose Failure can Contribute to Severe Overcooling Transients

Conduct a review of the automatic and manual control systems and identify all systems that have the potential for contributing to severe overcooling transients in the primary system of sufficient magnitude to initiate re-pressurization via the emergency core cooling system (ECCS). Determine the potential impact of each of the systems that are identified and establish the order of importance of these systems. Document the systems whose failure or malfunction may be considered less important or inconsequential to warrant any further study and document the basis for such action. During this stage the criteria that will be used for selecting and categorizing the safety significance of control systems will be defined. This screening criteria will primarily be developed with assistance from Task A-49. This assistance will be in defining important event sequences and describing unacceptable pressure-temperature conditions that could occur as a result of selected control system failures. Gross analytical techniques such as qualitative FMEA and event trees on a system level basis will be used to identify these control systems. During this phase, non-mechanistic "worst-case" failure modes of the systems will be assumed In addition, the major components of these systems such as the valves, pumps, input sensors, etc., whose failure can cause system malfunction will also be identified.

As part of a separate sub-task conducted for Task A-49, RES has contracted ORNL (FIN No. B-0468) to perform a study of PTS, including as one sub-task, the control and safety system design for each of the three PWR vendors (the same plants will be used for this Task.) One purpose of the contract is to provide details of the control and safety functions that could contribute to pressurized thermal shock events. We plan to utilize the control system information developed on that sub-task and include their findings in our evaluation.

2.2 Identify System Failure Modes

Identify the failure mechanisms (i.e., causes) of the control systems that have been defined in sub-task 2.1. Mechanistic failures, such as short or open circuits, the loss of environmental support systems, the loss of power supply (see task 4), seismic effects and operator action will be evaluated during this phase to determine the need and the type of corrective action.

Additional FMEA and fault tree analysis will be performed on a component level for selected systems as needed. The need for additional analysis will be evaluated on a case-by-case basis. The relative importance of the control system, its complexity and its dependence on other systems will be a factor for implementing any additional analysis. During this phase, the review of the applicable portions of the sub-task described in task 4 (the effects of the loss of power supplies) will be conducted on those control systems designs identified in Section 2.1.

2.3 Conduct Computer Simulation Studies for Combination of System Failures

Develop an analytical model to simulate the reactor vessel overcooling transient, using existing codes whenever possible.

As part of the activities conducted at ORNL (FIN No. B-0467), RES will develop a generic model to simulate the dynamic behavior of a PWR type plant. Concurrently, as part of the activities conducted at EG&G Idaho (FIN No. A-6477) we plan to develop a generic model to simulate the dynamic behavior of a BWR type plant. These models will include the plant characteristics of the primary reactor fluid system and the secondary steam and feedwater system, as well as the modeling for the major elements of the control system. We plan to use these generic models, modify them as necessary to simulate the plant specific characteristics of the four plants under review and evaluate the transients that would occur as a result of system failures identified in sub-task 2.1. Appropriate combinations of these failed systems, in sequence and simultaneously will be evaluated in the simulation studies. It is anticipated that this tool will significantly minimize the need for extensive use of the analytical techniques that normally would be used to accomplish the tasks identified in sections 2.1 and 2.2 above.

2.4 Determine the Need for Control or Protection System Improvements

Evaluate the need (if any) for additional safety or non-safety grade equipment such as, alarms, controls, or interlocks or modification on the existing designs. Also, evaluate the need for additional improvements on the existing control or electrical power system on the control systems identified in Section 2.1. The need for additional or improved operator action should be considered during this phase. Evaluate the effectiveness and the merits of each types of design improvement and establish the basis for a selection preference (i.e., high reliability, cost effectiveness, etc.). Coordinate these activities with Task Action Plan A-49 and integrate any necessary proposed requirements information data developed as a result of that activity.

2.5 Provide Design Criteria for the Evaluation of Control and or Protection Systems for Overcooling

Verify the adequacy of the existing criteria for control systems (Standard Review Plan Section 7.7) or if necessary develop and propose additional criteria or guidelines to improve system reliability and minimize control system failures that could lead to severe overcooling transients.

As a result of this study and at the completion of this task and Task A-49, the NRC staff will issue an evaluation and propose, if necessary, any modification to existing criteria of the system design. The report will contain recommendations for futher staff actions.

Task 3. EVALUATE (ALL OTHER) NON-SAFETY GRADE SYSTEMS THAT HAVE SAFETY IMPLICATIONS

This task will evaluate non-safety grade control systems and identify any non-safety grade control systems whose failure could lead to transients or accidents more severe than those evaluated in Chapter 15 of the plant FSAR. The same plants selected for review of Task 1 and Task 2 will also be used for this task. The control systems evaluation will review the designs of each of the four NSS suppliers (B&W, CE, W, and GE) and will include the control systems which may be designed by other suppliers but interface with the NSS control system design or dynamically interact with the reactor primary or secondary system. This task will consist of the following sub-tasks.

3.1 Identify the Systems Whose Failure can Lead to Significant Primary System Transients.

Conduct a review of the automatic and manual control systems that are used during start-up, shutdown and normal load varying operations and identify all systems whose failure or malfunction has the potential for causing pressure, temperature, and power transients in the primary reactor system. Compare the developed list with the systems identified in the analysis of Chapter 15 of the FSAR and determine the safety impact and the order of importance of the systems identified. Document the control systems whose failure or malfunction may be considered less important or inconsequential to warrant any further study and document the basis of such action. For example, there may be control systems whose failures produce transients that are enveloped by the limiting transients assumed in the Chapter 15 analyses, and therefore, failure

of these systems would be of little relative consequence. During this stage the criteria used for selecting and categorizing the safety significant control systems will be defined. Gross analyses based on tools such as FMEA, dependency tables or diagrams, functional and system event trees and fault trees and/or any other analytical tools judged to be adequate will be used on a system level basis for the purpose of identifying the significant control systems.

The analysis should be oriented toward identification and evaluation of the impact of system interaction and failure dependencies.

During this phase, non-mechanistic "worst-case" failure modes of the systems will be assumed. In addition, the major components of concern such as the valves, pumps, level transmitters, etc., whose failure can cause the specific system malfunction will be identified.

3.2 Identify System Failure Modes

Identify the failure mechanisms (i.e., root causes) of the control systems that have been defined in sub-task 3.1. Mechanistic failure, such as short and open circuits, the loss of environmental support systems, the loss of power supply (see task 4), seismic effects and operator action will be evaluated during this phase in order to determine the need for and the type of corrective actions. Additional FMEA and fault tree analysis will be performed on a component level for selected systems as needed. The need for quantitative analysis will be evaluated on a case-by-case basis. The relative importance of the control system, its complexity and its dependence on other systems will be a factor for implementing any additional analysis.

The data base for the logic fault and event tree analysis will be identified, and will indicate which portion is generic and plant specific. Sensitivity analysis (importance analysis) will be conducted to provide a basis for ranking the control systems and the components within each system for evaluating design modifications (if any) within each control system. During this phase, the review of the applicable portions of the sub-tasks described in task 4 (the effects of loss of power supplies) will be conducted on those control system designs identified in Section 3.1.

3.3 Conduct Computer Simulation Studies For Combination of System Failures

Develope an analytical model to simulate the reactor transients as a result of control system failures or malfunctions, using existing codes whenever possible. As part of the activities conducted at ORNL (FIN No. B-0467), RES will develop a generic model to simulate the dynamic behavior of a PWR type plant. Concurrently, as part of the activities conducted at EG&G Idaho (FIN No. A-6477) we plan to develop a generic model to simulate the dynamic behavior of a BWR type plant. These models will include the plant characteristics of the primary reactor fluid system and the secondary steam and feedwater system, as well as the modeling for the major elements of the control systems. We plan to use these generic models, modify them as necessary to simulate

the plant specific characteristics of the four plants under review and evaluate the transients that would occur as a result of the system failures identified in sub-task 3.1. During this phase an assessment will be made as to the possibility of utilizing any other dynamic models in part or in whole, already developed by others to simulate the plant specific characteristics of the plants under review. For example, the benefits of using the models developed for the LOFT project, or the use of the Tennsessee Valley Authority (TVA) simulators, or the capability to use the NSS vendor engineering simulators will be evaluated. The necessary modeling for this sub-task will be completed and conducted simultaneously with the modeling efforts described in sub-tasks 1.3 and 2.3. Appropriate combinations of the failed systems identified in sub-task 3.1, in sequence and simultaneously, will be evaluated in these simulation studies. It is anticipated that this tool will significantly minimize the need for extensive use of other analytical techniques that normally would be used for the tasks identified in section 3.1 and 3.2 above.

3.4 Determine the Need for Control or Protection System Improvements

Evaluate the need for additional non-safety grade controls, or the need for additional safety grade protection functions, the need to improve the reliability of the existing control and power systems and the adequacy of sharing common sensor lines between safety and non-safety systems. Review the activities and approaches used by the international community on how they improve control system reliability and minimize control system failures. Also, the need for improved or additional operator actions should be considered during this pahse. Assess the benefits, the feasibility and the need to require periodic surveillance testing and/or selective replacement of components on non-safety grade control systems as a means of improving control system reliability. Cost benefit analysis will be performed to evaluate the merits of any approaches recommended.

Applicable information data developed by other on going NRC activities conducted by 1) RES through contracts with ORNL and Sandia, 2) Instrumentation and Control Systems Branch (ICSB) case reviews, 3) the RRAB System Interaction Study for Indian Point Unit #3 and 4) the IREP Study for Calvert Cliffs 1, Millstone 1, Arkansas Nuclear One Unit 1 and Browns Ferry Unit 1 will be assessed as part of this sub-task. The data developed from these activities that identifies significant control systems and assesses their reliability will be considered in the evaluation of this Task.

3.5 Provide Design Criteria for the Evaluation of Control Systems

Verify the adequacy of the existing criteria for control systems (Standard Review Plan 7.7) or if necessary develop and propose additional criteria or guidelines to improve system reliability and minimize control system failures that could lead to a transient more severe than predicted in the plant FSAR accident analyses.

As a result of this study and at the completion of this task, the NRC staff will issue a draft NUREG Report describing the conduct and

conclusions of the task identified above (including task 4) including proposed recommendations for control system modifications (if any). Public comments on the draft report will be solicited and the comments addressed before issuing a final report.

Task 4. EVALUATE THE EFFECTS OF LOSS OF POWER SUPPLY TO THE CONTROL SYSTEMS. (Including electric (AC & DC) pneumatic, and hydraulic power sources.)

Numerous incidents have occurred in Nuclear Generating Plants involving loss of power in the non-safety grade instrumentation and control systems. These incidents resulted in: reactor and turbine trip, the opening of the pressurizer power operated relief valves, and code safety valves; discharge of a significant amount of primary coolant into the containment building and the loss of display instrumentation in the control room. The transients and the loss of equipment function produced as a result of these incidents significantly impact the operators ability to proceed to safe shutdown conditions in an orderly manner. The purpose of this task is to evaluate the effects of loss or degradation of the safety grade, non-safety grade power supplies which provide power to the non-safety grade instrumentation and control system. The evaluation will include the effects of the loss of AC and DC electrical power sources and loss of any applicable pneumatic and hydraulic power sources that operate any important valves. The evaluation will be limited to the loss or degradation of a single power supply and multiple power supply failures that result from a single (source) failure or event. The control systems of the four plant designs as described in each of the tasks will be reviewed. The review of this task will be integrated as part of a review effort associated with task 1, 2, and 3, respecitively. This task will consist of the following sub-tasks.

4.1 Coordinate activities with the findings of USI A-44, "Station Blackout," and NUREG-0666 (Ref. 10), and integrate any applicable requirements and information developed as a result of that activity.

4.2 Consider in the licensees evaluation and responses to IE Bulletin 79-27 (Ref. 3). This subtask will complement the review of Bulletin 79-27 and evaluate AC and DC bus power supply failurup to and including the 13KVA or 6.9 KVA bus failures, on important non-safety equipment and systems. If the non-safety grade equipment is powered from a safety bus, the effects of bus degradation on the safety loads connected on that bus will also be evaluated.

4.3 Identify and document the control system that have a significant safety impact due to power supply failures (this will be a specific subgroup of the systems identified in Section 2.1, and 3.1. Evaluate the effects of a loss of power to the display instrumentation of these systems. Using the criteria and guidance proposed in Reg. Guide 1.97 Rev. 2 "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant and Environment Conditions During and Following an Accident." Determine to what extent the problems found would be resolved by implementing this guide. Verify the adequacy of existing criteria or develop additional criteria (if necessary) to minimize the consequence of such power failures. Assess the reliability of the non-safety grade electrical bus, by evaluating the existing operating history. The effects of the non-safety grade bus failures during start-up, shutdown, normal power operation and during accident and transient modes of operation will be considered in the evaluation.

4.4 Develop and propose criteria (or guidelines) to improve the reliability of non-safety grade power supplies (if necessary) and propose recommendations to improve the capability of the systems to cope with the effects of the system failures identified in sub-task 4.3. Integrate the applicable requirements and information developed as a result of the IREP studues conducted on Calvert Cliffs 1, Millstone 1, ANO-1 and Browns Ferry 1, and those identified in sub-task 4.1. In addition, integrate the applicable information that is developed as a result of the Sandia studies (FIN No. A-1324).

3. BASIS FOR CONTINUED OPERATION OR LICENSING PENDING COMPLETION OF PROGRAM

As previously noted, the NRC staff has performed instrumentation and control system reviews on licensed plants and is currently reviewing on a case-by-case basis, the NTOL plants. The goal of the reviews is to verify that the control system failures (either single or multiple failures) will not prevent automatic or manual initiation and operation of any safety protection system equipment required to trip the plant or maintain the plant in a safe shutdown condition following any "anticipated operational occurrence" or "accident." These reviews are performed utilizing, in whole or in part, the guidelines and criteria identified in the Standard Review Plan (NUREG 75-087) Section 7.7.

With the recent emphasis on the availability of post-accident instrumentation (Ref. 7), the staff reviews evaluate the designs to assure that control system failures will not deprive the operator of information required to maintain the plant in a safe shutdown condition after any "anticipated operational occurrence or accident." For the NTOL reviews, the applicants are requested to evaluate their control systems and identify any control system whose malfunction could impact plant safety. The licensees are requested to identify the use (if any) of common power supplies, and the use of common sensors or common sensor impulse lines whose failure could have potential safety significance. The results of these reviews and the staff's evaluation for the NTOLs are documented in the Safety Evaluation Reports on a case-by-case basis.

In addition, a specific set of "accidents" has been analyzed to demonstrate that plant trip and/or safety system equipment actuation occurs with sufficient capability and on a time scale such that the potential consequences to the health and safety of the public are within acceptable limits. In these analyses, conservative assumptions have been used. The conservative analyses performed and the "accidents" chosen for the analyses are intended to demonstrate that the potential consequences to the health and safety of the public are within acceptable limits for a wide range of postulated events even though specific actual events might not follow the same assumptions made in the analyses.

Several activities that have been completed or are still ongoing which address the effects of control system failures have been conducted by the NSS vendors. B&W has completed a failure modes and effects analysis and a review of operating experience for their Integrated Control System (ICS) and reported the results in B&W Report BAW-1564 (Ref. 2). The staff completed its review of BAW-1564 through a technical assistance contract with Oak Ridge National Laboratory (ORNL) (Ref. 5). As a result of this review, both the staff and ORNL concluded that the ICS itself had a relatively low failure rate and did not appear to initiate a significant number of plant upsets. Failure statistics revealed that only approximately 6 of 162 hardware malfunctions resulted in reactor trip. ORNL has further concluded that the B&W analysis shows that anticipated failures of and within the ICS are adequately mitigated by the plant safety systems and many potential failures would be mitigated by cross checking features of the control system without challenging the plant safety systems. In BAW-1564, B&W recommended six actions regarding control system improvements which could be made to improve overall plant performance. In November 1979, the licensees with B&W plants (except Three Mile Island Unit 1) were requested to evaluate the B&W recommendations and report their follow-up actions. [Responses are currently being reviewed by ICSB.]

Also, the licensees have been requested (Ref. 4) to review the possibility of consequential control system failures which exacerbate the effects of high energy line breaks (HELB) and adopt design changes or new operator procedures where needed, to assure that the postulated events would be adequately mitigated. All licensees responded to the request and the responses were screened. On the basis of the review, no specific event leading to unacceptable consequences was identified and, in general, control equipment locations were such that consequential failures would be unlikely. Some licensees did make changes to their operating procedures to address the possibility of control failures. As part of the staff's on going review of the adequacy of the equipment qualification program on NTOLs, and in response to IE Bulletin 79-01 (Ref. 1) for all operating reactors, the staff is re-evaluating the qualification programs to assure that equipment that may potentially be exposed to HELB environments have been adequately qualified or an adequate basis has been provided for not qualifying the equipment to the limiting hostile environment.

The equipment qualification evaluations are conducted on a case-by-case basis. The staff reviews for all operating plants will be documented in the supplemental Safety Evaluation Reports. For NTOLs, the staff reviews will be completed before operating licenses are granted.

In addition, IE Bulletin 79-27 (Ref. 3) was issued to licensees requesting that evaluations be performed to ensure the adequacy of plant procedures for accomplishing shutdown upon loss of power to any electrical bus supplying power for instruments and controls. In their responses to the Bulletin, licensees have indicated that

corrective action has been taken including hardware changes and revised procedures, where required, to assure that the loss of any single instrument bus would not result in the loss of instrumentation required to mitigate such an event. As part of OL licensing reviews, ICSB is requesting that similar reviews be conducted by the NTOL applicants.

Based on the activities identified above and the on going NTOL case review activities, continued licensing and operation of PWRs and BWRs is acceptable pending completion of this program.

4. NRC TECHNICAL ORGANIZATIONS INVOLVED

A. Division of Licensing (DL)

Provides the coordination necessary to expedite and collect system design information on four operating reactors. The information needs will be to procure system piping and instrumentation designs and flow and logic diagrams for the non-safety grade control systems. Associated control equipment support system design schematics, such as power supply systems, will also be needed. DL will provide assistance to the Task Manager for setting up and coordinating with the utility personnel, information meetings and site visits that may be necessary. DL will also provide assistance to the Task Manager for integrating any relevant experience and any new requirements resulting from the activities identified in Task A-47. DL will contribute to the review and approval of any licensing requirements and guidelines developed as a result of this Task, and will provide review and comment on the technical evaluations provided by the Task Manager.

Manpower Requirements

	Total	FY82	FY83
Operating Reactors Branch No. 1	0.20 my*	.05	.15
Operating Reactors Branch No. 3	0.20 my	.05	.15
Operating Reactors Branch No. 4	0.20 my	.05	.15
Licensing Branch No. or	0.20 my	.05	.15
Operating Reactors Branch No. 2	0.20 my	.05	.15
Operating Reactor Assessment Branch	0.30 my	.10	.20

B. Division of Systems Integration,(DSI)

Provides review and comment on technical evaluations provided by the Task Manager in the areas of instrumentation and control, electrical power, the reactor and auxiliary plant designs, and accident analysis. The Instrumentation and Control Systems Branch and the Power Systems Branch will provide assistance for the purpose of integrating relevant experience and any new requirements and guidelines stemming from the completion of the sub-tasks described

---

Assumed 1 man year = 40 man weeks.

in Task A-47. The Reactor Systems Branch and the Auxiliary Systems Branch will assist in the development of the selection criteria to be used for establishing safety significant control systems (described in sub-tasks Sections 1.1, 2.1 and 3.1) and will verify completeness of non-safety grade control systems that may be needed in mitigating the accidents and transients analyzed in Chapter 15 of the plant FSAR. In addition DSI will contribute to the formulation, review and approval of the recommendations, and guidelines developed at the completion of the tasks (described in Task A-47). DSI will also review and comment on the draft and final NUREG Report.

Manpower Requirements

	Total	FY82	FY83
Instrumentation and Control Systems Branch	0.35 my	.05	.30
Power Systems Branch	0.25 my	.05	.20
Reactor Systems Branch	0.50 my	.10	.4
Auxiliary Systems Branch	0.175 my	.05	.125

C. Division of Human Factors Safety (DHFS)

Provides review and comment on those technical evaluations involving man/machine interfaces. DHFS will contribute to the formulation, review and approval of recommendations and guidelines involving man/machine interfaces developed at the completion of the tasks. In this area DHFS will contribute in the development of maintenance or testing requirements (if warranted) for non-safety control systems.

Manpower Requirements

	Total	FY82	FY83
Human Factors Engineering Branch	.15 my	0	.15
Procedures and Test Review Branch	.15 my	0	.15

D. Division of Safety Technology (DST)

Provides overall management of the program to resolve this USI. Provides liaison between NRR and RES and provides coordination of activities performed within NRR which are part of this Task Action Plan. DST has primary responsibility for the review of the draft recommendations and guidelines and for coordination of the internal management and the public review process required to adopt the recommendations and guidelines into licensing requirements. DST will provide review, comment and technical support on those issues/evaluations provided by the Task Manager involving reliability and risk assessments, and cost benefit assessments related to non-safety control systems.

DST will provide assistance to the Task Manager for the purpose of integrating relevant experience and any new requirements stemming from the completion of those activities related to Task A-47 for which DST has responsibility. Those activities include RRAB System Interaction Studies, and the Task A-49 and Task A-44 activities referenced in previous sections of this plan.

In addition, the Reliability and Risk Assessment Branch (RRAB) will provide technical support in the area of reliability and risk assessments on non-safety control systems that have been identified as safety significant. The Safety Program Evaluation Branch (SPEB) will provide technical support on the cost/benefit evaluations associated with the recommendations and positions developed on each of the sub-tasks. DST will also coordinate the revision and publication of the NUREG Report and coordinate the issuance of other licensing documents such as Regulatory Guides, Rules, and the Standard Review Plan with the Division of Engineering Technology.

Manpower Requirements

	Total	FY82	FY83
Generic Issues Branch	2.25 my	.75	1.50
Reliability and Risk Assessment Branch	.3 my	.075	.225
Licensing Guidance Branch	.15 my	.05	.10
Safety Program Evaluation Branch	.3 my	.00	.3
Research & Standards Coordination Branch	.15 my	.05	.10

E. Office of Analysis and Evaluation of Operational Data (AEOD)

Provides review and comment on the technical evaluations provided by the Task Manager. AEOD will provide assistance to the formulation, review and comment of the recommendations and guidelines developed (primarily on tasks 1 and 3). AEOD will also provide assistance to the Task Manager for the purpose of integrating relevant experience for which AEOD has responsibility.

Manpower Requirements

	Total	FY82	FY83
Plant Systems Unit	.15 my	.05	.10

5. ASSISTANCE FROM RES DIVISIONS

Close coordination and cooperation will be required on Task A-47 between NRR and RES. RES assistance will be required from the Division of Facility Operations, Instrumentation and Control Research Branch (ICRB). ICRB through contracts with ORNL, will develop the generic PWR simulator models (discussed in Sections 1.3, 2.3 and 3.3) as a specific input for the activities outlined in Task A-47. In addition RES (FIN No. B-0467) will conduct a review on two of the three PWR designs discussed in TAP A-47 and will perform the activities identified in Task 1, 2, 3, and 4 on each of these plants in conformance with the schedule identified in Figure 1. RES will also provide a draft report on each of the two plants reviewed. The report will include the content of the information described in Sections 1.5, 2.5 and 3.5.

Any control systems identified by RES to be generic will be identified in Task A-47. In addition the Division of Risk Analysis will provide technical input from Task A-44, "Station Blackout" relative to loss of power to the vital buses associated with non-safety control systems. Also, any applicable information developed by the Sandia plant electrical systems study (FIN No. A-1324) that would enhence a more complete understanding of significant interactions between the electrical power and the electrical control systems will be factored into the overall evacuation if the information is available and compatable with the schedule for resultion of this task.

Manpower Requirements

	Total	FY82	FY83
Instrumentation and Control Research Branch	.70 my	.4	.30
Division of Risk Analysis	.225 my	.075	.15

(The manpower requirements for RES/ORNL activities are summarized in Table 1).

6. TECHNICAL ASSISTANCE

Technical assistance to the program will be required for tasks 1, 2, 3 and 4. Contracts will be made with the National Laboratories to conduct the studies and activities described in Section 2 of this Plan. Funding will be provided by the Office of Nuclear Reactor Regulation and the Office of Nuclea Regulatory Research. The estimated costs associated with tasks 1 through 4 are shown in Table 1. The proposed schedule for Task resolution is shown in Figure 1. Should additional evaluations of other plant designs be needed, a significant cost increase will take place. Such costs are not included in the cost estimates shown in Table 1.

The funding associated with the RES activities related to Task A-47, (specifically FIN No. B-0467 and FIN No. B-0468) are funded directly by the Division of Facility Operations, Office of Nuclear Regulatory Research. These related activities are a part of a large overall research program which is beyond the scope of Task Action Plan A-47.

7. INTERACTIONS WITH OUTSIDE ORGANIZATIONS

Interaction with outside organizations will include the NSS vendors, utilities, the architect/engineers, the Electric Power Research Institute, EPRI, ORNL, Sandia Laboratories, and EG&G-Idaho.

The activities of Task A-47 will be coordinated with the appropriate ACRS subcommittee. Significant information will be provided to the subcommittee as it becomes available and meetings will be scheduled at appropriate times. Peer review will be conducted through ACRS briefings and by establishing a peer review panel (if necessary) selected from outside NRC having appropriate expertise. In addition, as sub-task 3.4 progresses, it will be necessary to establish a strong interaction and information exchange with the international community. Attendance at international conferences and/or site visits to selected foreign utility agencies and consultants is anticipated.

8. POTENTIAL PROBLEMS

A. Traditionally, the licensees were not required to provide design and operating experience on non-safety grade control systems, and therefore complete information on the final "as built design" for these systems (i.e., schematics, flow logic diagrams and system descriptions) and operating experience may be difficult to obtain.

B. Performance of selected sub-tasks described in tasks 1 through 4 by NRR will require participation from members of DSI, DL, and RES at various intervals throughout the program. Unconditional assignments of selected personnel, at specific intervals, will be required. Close coordination and cooperation is needed within NRR (e.g., Task A-49) and between NRR and RES (e.g., ORNL).

C. Development of appropriate reliability/safety goals for specific non-safety grade control systems and translation of these goals into licensing requirements.

D. Uncertainty as to the applicability or compatability of the information that will be available from IREP, systems interaction studies, and other on going reliability and risk assessment studies for use on Task A-47. The completion schedules of these activities may not be compatible with Task A-47. Uncertainty as to whether the information obtained from these activities can be used for a generic study.

TABLE 1
A-47 USI FUNDING

	FY 1982		FY 1983		Total	
	Manpower	cost	Manpower	cost	Manpower	cost
EG&G Activities: Resolution of Task 1, 2, 3, and 4 of TAP A-47 review one BWR type design.	20MM	$170,000	24MM	$290,000	35MM	$360,000
EG&G or ORNL Activities (to be decided) Resolution of Task 1, 2, 3, and 4 of TAP A-47 on one CE, PWR design.	2MM	20,000	30MM	250,000	32MM	315,000
RES. (ORNL) activities (FIN No. B-0467) to include resolution of Task 1, 2, 3, and 4 of TAP A-47 on 2 PWR type designs.	60MM	600,000	60MM	600,000	120MM	1,200,000

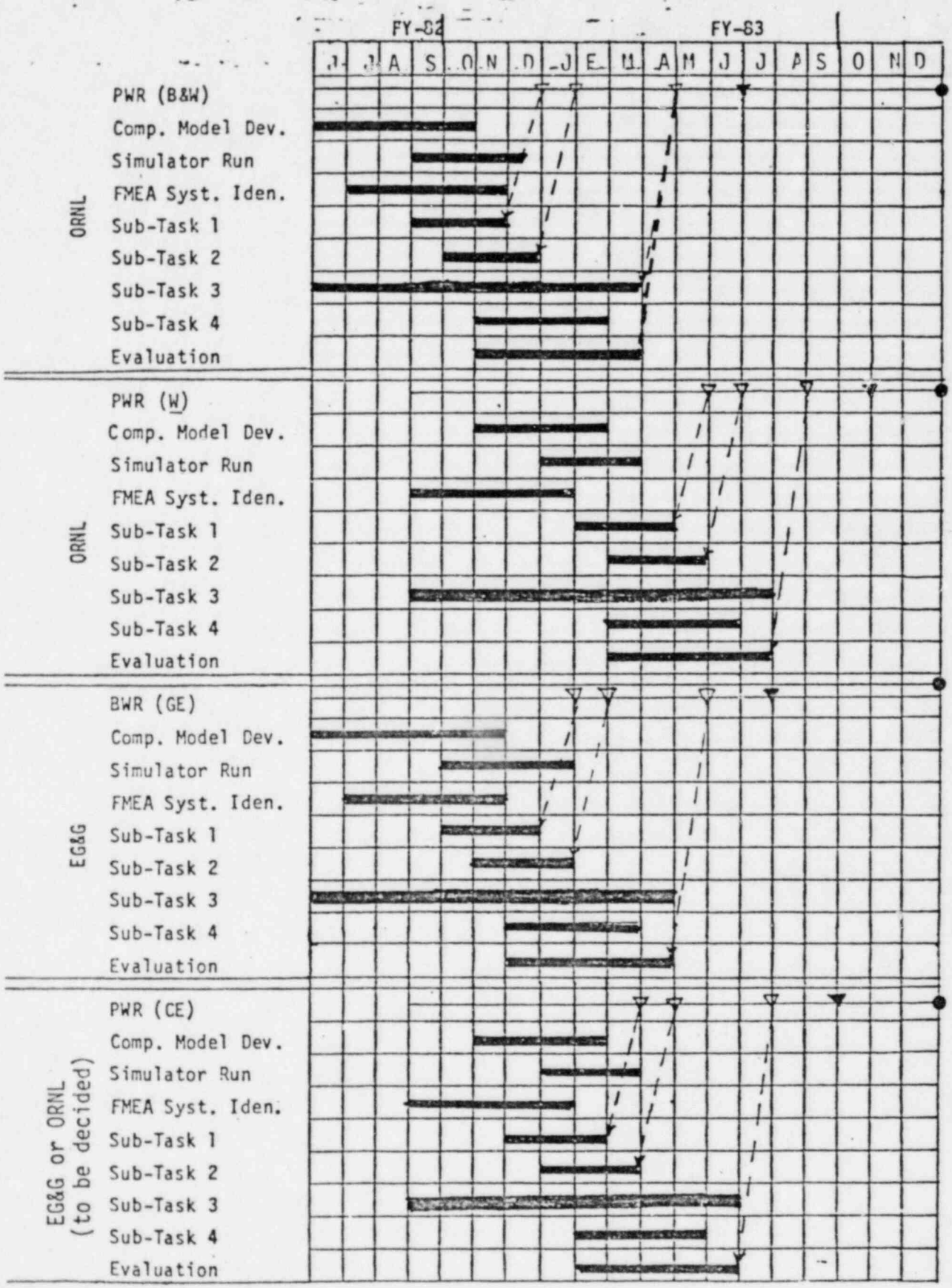
TABLE 2
RELATED ACTIVITY FUNDING

	FY 82 Cost	FY 83 Cost
RES (Sandia) Activities FIN No. A-1324	$350,000	$400,000

Figure 1

Proposed Schedule for Task A-47

"SAFETY IMPLICATIONS OF CONTROL SYSTEMS"



NOTE: Task 3 of TAP A-47 is everything outside of Tasks 1 & 2, and represents the bulk of the work of the activities identified above.

▽ Draft Report Submitted by Labs
▼ Final Report Submitted by Labs
● Draft Report Submitted by NRR

9. REFERENCES

1. NRC Bulletin 79-01, "Environmental Qualification of Class IE Equipment," February 8, 1979.

2. BAW-1564, Babcock and Wilcox report, "Integrated Control System Reliability Analysis," August 1979.

3. NRC Bulletin 79-27, "Loss of Non-Class IE Instrumentation and Control Power System Bus During Operation," November 30, 1979.

4. IE Information Notice 79-22, "Qualification of Control Systems," September 14 and 17, 1979.

5. Memorandum, R. Satterfield to P. S. Check, "Assessment of B&W Report 1564, 'Integrated Control System Reliability Analysis'," May 9, 1980.

6. Memorandum, H. Denton to J. F. Ahearne, "ACRS and AEOD Comments Concerning New Unresolved Safety Issues," September 10, 1980.

7. Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident," Revision 2, December 1980.

8. NUREG-0705, "Identification of New Unresolved Safety Issues Related to Nuclear Power Plants (Special Report to Congress)," March 1981.

9. Letter, J. Carson Mark to J. M. Hendrie, "Response to Inquiries Concerning the Safety Implications of Control System Failures," May 12, 1981.

10. NUREG-0666, "A Probabilistic Safety Analysis of DC Power Supply Requirements for Nuclear Power Plants," April 1981.

11. Memorandum, F. Rosa to W. Kerr, "Licensing Criteria for Control Systems in Foreign Countries," May 18, 1981.

12. Memorandum, A. J. Szukiewicz to T. E. Murley, "Activities Related to Task A-47, Safety Implications of Control Systems," September 24, 1981.